Math 6170 C, Lecture on March 16, 2020

Yongchang Zhu

Plan.

(1) Review of Chapter III § 3.

(2) Chapter III § 4.

Reivew of III § 3.

Proposition III 3.1. Let (E, O) be an elliptic curve defined over K. There exist functions $x, y \in K(C)$ such that the map

$$\phi : E \to \mathbb{P}^2 : \qquad \phi(P) = [x(P), y(P), 1]$$

gives an isomorphism of E/K onto a curve given by a Weierstrass equation

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

with coefficients $a_1, \ldots, a_6 \in K$ and such that $\phi(O) = [0, 1, 0]$.

Lemma 3.3.

Let E be a curve of genus one, $P, Q \in E$, then $(P) \sim (Q)$ iff $P = Q$.

Proposition III 3.4.

The abelian group E and $\mathrm{Pic}^0(E)$ are isomorphic. The isomorphism $\kappa : E \to \mathrm{Pic}^0(E)$ is given as

$$P \mapsto \text{class of } (P) - (O).$$

The proof needs the following result:

$$V \stackrel{\text{def}}{=} \{aX + bY + cZ \mid a, b, c \in \bar{K}\}$$

For each $0 \neq f = aX + bY + cZ \in V$, $P \in E$, we define $\mathrm{ord}_P f$ as follows.

We choose $g \in V$ such that $g(P) \neq 0$, then $f/g \in \bar{K}(E)$,

$$\mathrm{ord}_P(f/g)$$

is independent of the choice of g, we define

$$\mathrm{ord}_P f \stackrel{\text{def}}{=} \mathrm{ord}_P(f/g).$$

It is easy to see that for almost all $P \in E$, $\mathrm{ord}_P f = 0$.
We define

$$\mathrm{div}(f) = \sum_{P \in E} \mathrm{ord}_P f \ (P)$$

$$\mathrm{div}(f) \in \mathrm{Div}(E).$$

We have for $f, g \in V$, both are not 0,

$$\mathrm{div}(f) - \mathrm{div}(g) = \mathrm{div}(f/g).$$

Lemma. If $0 \neq f = aX + bY + cZ$ and the line $L : aX + bY + cZ = 0$ intersects to E at P, Q, R (counting with multiplicity), then

$$\operatorname{div} f = (P) + (Q) + (R).$$

This lemma is used to prove $\kappa : E \to \mathrm{Pic}^0(E)$ is a group homomorphism.

Theorem 3.6

Let (E, O) be an elliptic curves over K, then

$$+ : E \times E \to E, \quad - : E \to E$$

are morphisms of variety.

Proof. The formula for $-$ shows that $-$ is a rational map defined on an open subset of E. Because E is a smooth curve, by Proposition II 2.1, $-$ extends to whole E.

Proof of Theorem 3.6 (continued).

Note that for any given $a \in E$, the translation map $T_a : E \to E, x \mapsto x + a$ is a rational map, by Proposition II 2.1, T_a extends to whole E.

The formula for $+$ shows that $+$ is a rational map defined on an open subset $U \subset E \times E$.

$$\phi_{a,b} \stackrel{\text{def}}{=} T_{-a-b} \circ (+) \circ (T_a \times T_b) : E \times E \to E$$

is a rational map defined by $U - (a, b)$.

$\phi_{a,b} = \phi_{a',b'}$ on $(U - (a, b)) \cap (U - (a', b'))$, the union of all $U - (a, b)$ is $E \times E$. So $+$ can be extend to all $E \times E$.

Definition. Let E_1 and E_2 be elliptic curves. An **isogeny** between E_1 and E_2 is a morphism $\phi : E_1 \to E_2$ such that $\phi(O) = O$.

E_1 and E_2 are **isogeneous** if there is an isogeny ϕ between them with $\phi(E_1) \neq \{O\}$.

Let

$$\mathrm{Hom}(E_1, E_2)$$

be the set of isgenies $\phi : E_1 \to E_2$.

$\mathrm{Hom}(E_1, E_2)$ is a group under the addition law:

$$(\phi + \psi)(P) = \phi(P) + \psi(P).$$

$\mathrm{End}(E) = \mathrm{Hom}(E, E)$ has a ring structure with multiplication given by composition.

If elliptic curves are defined K, we use subscripts K to denote the set of isogenies over K:

$\mathrm{Hom}_K(E_1, E_2)$ is the set of isogenies from E_1 to E_2 over K.

$\mathrm{End}_K(E)$ is the set of isogenies from E to itself over K.

For m a positive integer, we define

$$[m] : E \to E, \quad P \mapsto P + \cdots + P \ (m \text{ copies}).$$

We define $[0] : E \to E$ to be the constant map $P \mapsto O$.

For negative integer $-m$:

$$[-m] : E \to E, \quad P \mapsto -[m]P = -(P + \cdots + P) \ \ (m \text{ copies}).$$

$$[m][n] = [mn], \quad [m] + [n] = [m + n]$$

Proposition III 4.2.

(a) Let E be an elliptic curve and $m \in \mathbb{Z}$, $m \neq 0$. Then the multiplication by m map $[m]$ is non-constant.

(b) Let E_1, E_2 be elliptic curves, the group of isogenies $\mathrm{Hom}(E_1, E_2)$ is a torsion free $\mathbb{Z}$-module.

(c) Let E be an elliptic curve, then the endomorphism ring $\mathrm{Hom}(E)$ is an integral domain of characteristic 0

$\mathbb{Z}$ is a subring of $\mathrm{End}(E)$.

Theorem III 4.8.

Let $\phi : E_1 \to E_2$ be an isogeny. Then

$$\phi(P + Q) = \phi(O) + \phi(Q)$$

for all $P, Q \in E$. That is, ϕ is a group homomorphism.

Proof.

If $\phi = O$, there is nothing to prove. Otherwise ϕ is a finite map, it induces a homomorphism

$$\phi_* : \ \mathrm{Pic}^0(E_1) \to \mathrm{Pic}^0(E_2)$$

given by

$$\phi_*(\text{class of } \sum n_i(P_i)) = \text{class of } \sum n_i(\phi P_i)$$

See II.3.7. Recall we have group isomorphisms

$$\kappa_i : E_i \to \mathrm{Pic}^0(E_i)$$

$$P \mapsto \text{class of } (P) - (O)$$

Proof (continued).

We have commutative diagram:

$$
\begin{array}{ccc}
E_1 & \longrightarrow & \mathrm{Pic}^0(E_1) \\
\downarrow \phi & & \downarrow \phi_* \\
E_2 & \longrightarrow & \mathrm{Pic}^0(E_2)
\end{array}
$$

Let ϕ be a non-constant isogeny, Then

$$|\mathrm{Ker}(\phi)| = \deg_s \phi$$

So $\mathrm{Ker}(\phi)$ is a finite group.

Theorem 4.10.

Let $\phi : E_1 \to E_2$ be a non-constant isogeny.
(a) For every $O \in E_2$,

$$|\phi^{-1}(Q)| = \deg_s \phi$$

(b) The map

$$\operatorname{Ker} \phi \to \operatorname{Aut}(\bar{K}(E_1)/\phi^* \bar{K}(E_2))$$

given by

$$P \mapsto \tau_P$$

is an isomorphism.

(c) Assume that ϕ is separable. Then ϕ is unramified. And $\bar{K}(E_1)$ is a Galois extension of $\bar{K}(E_2)$ with Galois group isomorphic to $\mathrm{Ker}\,\phi$.

Proposition III 4.12.

Let E be an elliptic curve, and let Φ be a finite subgroup of E. Then there is a unique elliptic curve E' and a separable isogeny

$$\phi : E \to E'$$

such that

$$\ker \phi = \Phi.$$

Proof.

Φ acts on $\bar{K}(E)$. The fixed point field

$$\bar{K}(E)^{\Phi}$$

is a subfield of $\bar{K}(E)$. The extension $\bar{K}(E)^{\Phi} \subset \bar{K}(E)$ is a Galois extension with Galois group Φ.

In general, if F is a field, Φ is a finite subgroup of automorphisms of F, then $F^{\Phi} \subset F$ is a finite Galois extension with Galois group Φ.

Proof (continued).

$\bar{K}(E)^\Phi$ is a finitely generated field over $\bar{K}$ with transcendental degree 1 over $\bar{K}$. So it corresponds to a smooth curve C over $\bar{K}$.

The embedding $\bar{K}(E)^\Phi \subset \bar{K}(E)$ gives a morphism of curves

$$\phi : E \to C$$

with $\deg \phi = |\Phi|$.

Proof (continued).

It is clear that $\phi \circ \tau_a = \phi$ for every $a \in \Phi$. So $\phi^{-1}(b)$ is closed under the translation by τ_a with $a \in \Phi$.

$|\Phi| \leq |\phi^{-1}(b)| \leq \deg(\phi) = |\Phi|$

So

$$|\phi^{-1}(b)| \leq \deg(\phi)$$

Our map ϕ is unramified, separable.

Proof (continued). By Hurwitz formula (II 5.9), $\mathrm{genus}\, C = 1$.
$(C, \phi(O))$ is an elliptic curve.

Let E/K be an elliptic curve given by the usual Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

The differential

$$\omega = \frac{dx}{2y + a_1x + a_3} \in \Omega_E$$

has neither zeros nor poles.

Proposition 5.1

For ω as above, for every $Q \in E$,

$$\tau_Q^*\omega = \omega.$$

Proof.

$$\tau_Q^* \omega = f\omega$$

for some $f \in \bar{K}(E)^*$.

$$\mathrm{div}(\tau_Q^* \omega) = 0.$$

On the other hand side, we have

$$\mathrm{div}(\tau_Q^* \omega) = \mathrm{div}(f\omega) = \mathrm{div}(f) + \mathrm{div}(\omega) = \mathrm{div}(f).$$

So $\mathrm{div}(f) = 0$, $f \in \bar{K}^*$. We call this constant a_Q.

$a_Q \equiv 1$ for all Q.

Theorem III 5.2. Let E, E' be elliptic curves, let ω be an invariant differential on E, and let $\phi, \psi : E' \to E$ be two isogenies. Then

$$(\phi + \psi)^* \omega = \phi^* \omega + \psi^* \omega$$

End